Exhibit 8

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

22 MAG 1577

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR ORDER TO DISCLOSE NON-CONTENT INFORMATION PURSUANT TO 18 U.S.C. § 2703(d)

SEALED APPLICATION

Nicolas Roos affirms as follows:

1. I am an Assistant United States Attorney in the Southern District of New York and, as such, I am familiar with this matter.

2. The Government is seeking an Order pursuant to Title 18, United States Code, Section 2703(d) to require Google, LLC ("Google" or the "Provider"), to provide the to/from headers and other non-content information for e-mails stored in the following email accounts (the "Target Accounts"):[1]

Email Address	**Account Owner**	**Target Account #**
amonje@dwacspac.com	Alexander Monje	Target Account-1
ljacobson@dwacspac.com	Montie Jacobson	Target Account-2
jshaner@dwacspac.com	Justin Shaner	Target Account-3
eswider@dwacspac.com	Eric Swider	Target Account-4
rveloso@dwacspac.com	Veloso Rodrigo	Target Account-5
bgarelick@dwacspac.com	Bruce Garelick	Target Account-6
phillip.juhan@tmediatech.com	Phillip Juhan	Target Account-7
andy.litinsky@tmediatech.com	Andrew Litinsky	Target Account-8
wes.moss@tmediatech.com	Wesley Moss	Target Account-9
will.wilkerson@tmediatech.com	William Wilkerson	Target Account-10

[1] Based on my review of publicly-available domain lookup information, it appears that the email domains @dwacspac.com and @tmediatech.com are hosted by Google.

The records requested from the Provider are set forth below and in the accompanying proposed Order.

3. 18 U.S.C. § 2703(c) provides authority for a court to order an electronic communications service provider to disclose records or information not including the contents of communications without notice to the subscriber or customer, if the records are relevant and material to an ongoing criminal investigation.

4. Specifically, 18 U.S.C. § 2703(c)(1) provides in pertinent part:

> A government entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or a customer of such service (not including the contents of communications) . . . when the governmental entity–
> . . . .
> obtains a court order for such disclosure under subsection (d) of this section;
> . . . .

5. 18 U.S.C. § 2703(d), in turn, provides (in pertinent part):

> A court order for disclosure under subsection . . . (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation.

As specified in 18 U.S.C. § 2711(3), this Court is a court of competent jurisdiction under the Stored Communications Act because it has jurisdiction over the offenses being investigated, as defined below.

6. In addition, 18 U.S.C. § 2703(c)(3) provides:

> A governmental entity receiving records or information under [18 U.S.C. § 2703(c)] is not required to provide notice to a subscriber or customer.

7. Finally, 18 U.S.C. § 2705(b) authorizes the Court to issue an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify

any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. § 2705(b)(1)-(5).

The Requested Records are Relevant and Material to an Ongoing Investigation

8. On or about February 10, 2022, the Honorable Debra Freeman signed a warrant to search the contents of five Apple iCloud accounts and three Google email accounts based on facts set forth in the affidavit of Special Agent Marc Troiano of the Federal Bureau of Investigation. The affidavit of Special Agent Troiano is attached as Exhibit 1 and is incorporated herein by reference. The affidavit describes probable cause to believe that certain target subjects of the investigation have engaged in insider trading and/or made false statements to the United States Securities and Exchange Commission ("SEC"), in violation of Title 18, United States Code, Sections 2, 371, 1001, 1343, 1348, 1349 and Title 15, United States Code, Sections 77x, 78j(b) and 78ff and Title 17, Code of Federal Regulations, Section 240.10b-5 (collectively, the "Subject Offenses").

9. Specifically, as described in the affidavit, the FBI and the United States Attorney's Office for the Southern District of New York are investigating an insider trading scheme in securities of Digital World Acquisition Corporation ("DWAC"), a special purpose acquisition

company ("SPAC")[2], the shares of which were publicly traded on the Nasdaq stock market beginning on or about September 3, 2021. On or about October 20, 2021, DWAC and Trump Media & Technology Group ("Trump Media"), a media and technology company founded in February 2021 by former United States President Donald J. Trump, announced that they had entered into a definitive merger agreement that would combine the two entities, allowing Trump Media to become a publicly-traded company. The investigation relates to disclosures in public filings by DWAC, as well as trading in DWAC stock in September and October 2021 based on material non-public information about its planned merger with Trump Media. As set forth in the affidavit, there is probable cause to believe that Patrick Orlando, the chief executive officer of DWAC, and/or other employees or directors of DWAC made false statements in filings with the SEC by falsely stating that DWAC was not in negotiations with any SPAC target, even though DWAC was in negotiations with Trump Media and other entities at the time. Additionally, as described in the affidavit, there is probable cause to believe that Bruce Garelick, a DWAC director, and other individuals who appear to be affiliated with or known to Garelick purchased DWAC stock after learning non-public information about its planned merger with Trump Media, and sold the stock shortly after the merger was announced.

10. The requested records relating to the Target Accounts are relevant and material to an ongoing investigation. First, Target Account-1 through Target Account-6 are all hosted by the dwacspac.com email domain and appear to be used by directors of DWAC. The requested information for those Target Accounts is relevant and material to the insider trading investigation because header information is likely to reveal who members of DWAC's board were

[2] A special purpose acquisition company, also known as a "blank check company," is a publicly traded company created for the purpose of acquiring or merging with an existing private company, thus making it public without going through the traditional initial public offering process.

communicating with, including individuals who traded in DWAC's stock in advance of the publicly announced merger with Trump Media. Additionally, the requested information is relevant to the investigation into false statements to the SEC, because the requested information will indicate whether directors, officers, or employees of DWAC were communicating with individuals acting on behalf of Trump Media at or around the time DWAC stated in public filings that it was not having negotiations. Second, the users of Target Account-7 through Target Account-10 are directors and/or officers of Trump Media. The requested information for those Target Accounts is relevant and material to the insider trading investigation because it may reveal that certain individuals, such as Garelick, were communicating with Trump Media employees and therefore may have had material non-public information about the merger. Additionally, the requested information is relevant and material to the investigation into false statements to the SEC, because the requested information will indicate whether directors, officers, or employees of Trump Media were communicating with individuals acting on behalf of DWAC at or around the time DWAC stated in public filings that it was not having negotiations.

11. In addition to header information, the Government also requests device information, IP address information, and cookie and linked account information for each of the Target Accounts. Specifically:

a. *Device information:* Google frequently obtains information about the types of devices that are used to access accounts like the Target Accounts. Those devices can be laptop or desktop computers, cellular phones, tablet computers, or other devices. Individual computers or devices are identified by a number of different means, some of which are assigned to a particular device by a manufacturer and connected to the "hardware" or the physical device, some are assigned by a cellular telephone carrier to a particular account using cellular data or voice services, and some are actually assigned by the Provider to keep track of the devices using its services.

Those device identifiers include GUIDs or Global Unique Identifiers, phone numbers, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"). These device identifiers can then be used (a) to determine the other accounts that are accessed by the same device and thus likely by the same person at the Provider tracking that information, (b) to determine accounts accessed at other providers by that same device, (c) to determine whether any physical devices found in the course of the investigation were the ones used to access each of the Target Accounts.

b. *IP address information:* An IP address is generally used to route communications between a Provider and the Target Accounts. Providers of certain communication services also require the use of additional routing information to accompany message or other communication in order to route information to the user of a certain account. That is commonly referred to as "network address translation," which allows information traveling, for example, to a particular household to reach the correct device within that household; this is sometimes accomplished by assigning a particular "port" for communications going between a Provider and the Target Accounts. Large mobile telephone carriers sometimes use more sophisticated systems that are referred to as "carrier grade" network address translation. The network address translation information is relevant because it will assist the investigation in resolving which account on, for example, a mobile carrier was used to send and receive information between the Target Accounts and a Provider, which can then assist in identifying whose cellular telephone was being used when accessing the Target Accounts.

c. *Cookie and linked account information:* Google often use features to track the activity of users of its accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account like one of the Target Accounts. As noted above, one of the ways it does that is by using cookies. Because one of the purposes of the investigation is to determine all of the accounts and means of communication used by the subjects of the investigation, both to identify the subjects and to obtain evidence of their conduct under investigation, the order calls for Google to provide records sufficient to identify those other accounts.

12. In addition to the above information, the Government also requests a list of email addresses registered to the email domains dwacspac.com and tmediatech.com.

13. Based on the foregoing, the Government requests that the Court enter the proposed Order submitted herewith. The materials to be requested from the Target Accounts will be limited, to the extent they are dated, to those created, sent, received, modified, or deleted on or about December 11, 2020, for the reasons set forth in the affidavit.

Non-Disclosure and Sealing

14. The Government further requests, pursuant to 18 U.S.C. § 2705(b), that this Application and the proposed Order be sealed by the Court until such time as the Court directs otherwise, and that the Provider be ordered not to notify any person (including the subscriber associated with the Target Account) of the existence of the Order for a period of one year from the date of the Order, subject to extension if necessary. In this case, such an order would be appropriate because the attached Order concerns an ongoing criminal investigation, where the existence and scope of the investigation is not known to the targets of the investigation, the account holders are suspected of being involved in or associated with persons involved in the conduct under investigation, and disclosure of Order to the account owner or to any other person may alert

subjects or targets of the ongoing investigation. The targets of this investigation are known to use computers and electronic communications in furtherance of their activity and thus could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation. *See* 18 U.S.C. § 2705(b)(3). Moreover, certain of the targets are believed to travel internationally frequently. *See* 18 U.S.C. §§ 2705(b)(2), (5). Accordingly, there is reason to believe that notification of the existence of the attached Order will seriously jeopardize the investigation, including by giving targets an opportunity to flee or avoid prosecution, or tamper with evidence, including electronically stored information that is easily tampered with. Given the amount of time a criminal investigation commonly lasts and the particular circumstances presented here, the Government respectfully submits that one year is an appropriate delay of notice period for the Court to order.

15. I know from past experience that Google will request that the Government seek data related email addresses with an enterprise domain such as, @dwacspac.com and @tmediatech.com, which would include data relating to five of the Target Accounts, directly from the enterprises, pursuant to the U.S. Department of Justice Policy titled Seeking Enterprise Customer Data Held by Cloud Service Providers, December 2017, available at https://www.justice.gov/criminal-ccips/file/1017511/download. However, @dwacspac.com and @tmediatech.com appears to be owned or controlled by DWAC and Trump Media, respectively, and all the users are, or are closely associated with, Target Subjects of this investigation. As they are the apparent owners of the enterprises, or are involved in controlling them, notification would almost certainly mean they would be informed of the existence of this search warrant, which could cause them to delete, encrypt, or otherwise conceal the requested data. To the extent the enterprises have outside counsel, disclosure to outside counsel does not appear to be a viable option because, based on my understanding of professional responsibility rules, such counsel will be required to

report such a disclosure to the client. Additionally, it is my understanding that certain materials requested from Google cannot be obtained directly from the enterprise because enterprise account users cannot access or download certain types of data, including the types of data requested for the Target Accounts. Therefore, I respectfully request that the proposed order specifically require the Provider to produce enterprise data.

16. No prior request for the relief sought herein has been made.

17. I declare under penalty of perjury that the foregoing factual assertions are true and correct to the best of my knowledge and belief.

Dated: New York, New York
February 15, 2022

Nicolas Roos
Assistant United States Attorney
212-637-2421

Exhibit 1
Affidavit of Special Agent Marc Troiano

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of Warrants for All Content and Other Information Associated with Certain Email and iCloud Accounts Maintained at Premises Controlled by Google, LLC and Apple Inc., USAO Reference No. 2021R01007

22 MAG 1354

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

Agent Affidavit in Support of Application for Search Warrants for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

MARC TROIANO, Special Agent, Federal Bureau of Investigation ("FBI"), being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent with the FBI for approximately six years. I am assigned to a squad in the FBI's New York Field Office that investigates securities fraud and other white-collar offenses. During my tenure with the FBI, I have participated in the investigations of numerous frauds, including securities fraud and insider trading, and have conducted physical and electronic surveillance and the execution of search warrants, including email search warrants. Through my training, education, and experience, I have become familiar with the manner in which insider trading is committed.

B. The Providers, the Subject Accounts and the Subject Offenses

2. I make this affidavit in support of an application for search warrants pursuant to 18 U.S.C. § 2703 for all content and other information associated with the following email and cloud storage accounts (collectively, the "Subject Accounts") maintained by the internet service providers (the "Providers") set forth below:

Account Identifier	Account User	Provider	Subject Account #
DSID [redacted]4470	BRUCE GARELICK	Apple	Subject Account-1
DSID [redacted]8701	BRUCE GARELICK	Apple	Subject Account-2
DSID [redacted]0824	PATRICK ORLANDO	Apple	Subject Account-3
DSID [redacted]6292	GERALD SHVARTSMAN	Apple	Subject Account-4
DSID [redacted]5920	RAYMOND CORRAL	Apple	Subject Account-5
bruce.m45@gmail.com	BRUCE GARELICK	Google	Subject Account-6
ms@rocketonecapital.com	MICHAEL SHVARTSMAN	Google	Subject Account-7
ray@mosaicist.com	RAYMOND CORRAL	Google	Subject Account-8

The information to be searched is described in the following paragraphs and in Attachments A and B to the proposed warrants.

3. There is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of securities fraud and wire fraud relating to insider trading, conspiring to commit those offenses, aiding and abetting the commission of those offenses, making false statements to the Securities and Exchange Commission ("SEC"), making false and misleading statements in an SEC registration statement, and conspiring to defraud the SEC, in violation of Title 18, United States Code, Sections 2, 371, 1001, 1343, 1348, 1349 and Title 15, United States Code, Sections 77x, 78j(b), and 78ff and Title 17, Code of Federal Regulations, Section 240.10b-

5 (collectively, the "Subject Offenses"). This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Providers

4. I have learned the following about Google:

a. Google is a United States company that offers email services to the public. In particular, Google allows subscribers to maintain email accounts under the free email domain name gmail.com. Additionally, Google allows individuals and entities to maintain email accounts under enterprise or G Suite domain names. If a subscribing individual or enterprise customer controls a domain name, such as the domain name "xyzbusiness.com," Google enables the individual or enterprise subscriber to host any email address under this domain name (*e.g.*, "john@xyzbusiness.com"), on servers operated by Google. A subscriber using Google's services can access his or her email account from any computer connected to the Internet.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents*. Google allows subscribers to maintain email accounts under the domain name "gmail.com." Like other online email providers, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the

subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Contacts.* Google also allows subscribers to maintain the equivalent of an address book, called "Contacts," comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google's website).

v. *Web & App Activity, Search, Chrome, and Browsing History.* Google maintains a history of a subscriber's websites visited, devices used, applications (or "apps") used, Google search query history, Chrome usage, and browsing records. For some accounts, Google maintains "My Activity" records for a subscriber, which include records of web searches, image searches, video searches, news browsing, map activity, and analytics on the account.

vi. *Google Drive Content*. Google also provides account holders access to "Google Drive" which enables users to back up documents, images, chat history, emails, and other files. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

vii. *Google Docs*. Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called "Google Docs." Users can use Google Docs to create online documents that can be stored on or saved to the user's Google Drive.

viii. *Google Photos*. Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or "exif") data, and can include GPS location information for where a photo or video was taken.

ix. *Google Calendar*. Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

x. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in "chat" sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user's e-mail content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user's e-mail and chat content.

xi. *Google Voice*. Google Voice is a telecommunications service provided by Google over the Internet, and can be configured to be used to make phone calls between computers, using voice over IP ("VoIP") connections, or can be configured to be used from existing cellular telephone devices. Google Voice users register Google Voice accounts to an existing Google email account. Users have the ability to configure their Google Voice account to accept calls to an existing landline or cell phone number, or to purchase new telephone numbers, as long as they are available, for a fee from Google. Users can use Google Voice to send or receive SMS messages, commonly referred to as "text messages." A Google Voice user can send a text message from a computer to any cellular telephone, and any text messages which are received by the Google Voice account are available in the user's email inbox, in the account linked to the Google Voice account. Google offers a voicemail service for Google Voice customers. When an incoming call to a Google Voice number is unanswered, the caller may leave a voice message. A copy of the recording, as well as a transcription of the recording are forwarded to the Google Voice user's email account that is linked to the Google Voice account.

xii. *Location History data*. Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or "apps") or services provided by Google. For example, Google collects information collected from GPS, Wi-

Fi networks, cell site locations, and mobile networks to estimate a user's location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

xiii. *Google Payments*. Google allows for the storage of payment information associated with a Google account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

xiv. *Device Information.* Google collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

xv. *Linked Accounts.* Google maintains records of whether the user of an account has other accounts that share the same recovery SMS number or secondary email address. Google also uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways it does that is by using cookies, a string of characters stored on the user's computer or web browser that is recognized by Google when a computer visits Google's site or logs into an account.

xvi. *Android Device Backups*. Android device users can use Google Drive to backup certain data from their devices. By default, Google regularly backs up the following data from Pixel phones (which are phones made by Google that use the Android operating system) to its online servers: smartphone application data, call history, device settings, contacts, calendar, SMS, photos, and video. For users that subscribe to Google's cloud storage service, Google One, they can opt to back up all the data from their device to Google Drive.

5. I have learned the following about Apple:

a. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system. Apple provides email services to its users through email addresses at the domain names mac.com, me.com, and icloud.com. Apple provides users with gigabytes of free electronic storage space on its cloud-storage platform iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may be used to store iOS device backups, which by default happen automatically for a user of an iCloud account. iCloud accounts may also be used to store or backup data associated with the use of iCloud-connected services including email (iCloud mail), images and video (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud accounts are accessed using an "Apple ID," which is typically created during the setup of an Apple device or through the registration of an iCloud account. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism. When an account is designated by Apple as a "full iCloud" account, it has been linked to one or more Apple devices. Because iCloud accounts are

typically linked to at least one iPhone, iCloud accounts are generally registered with a telephone number belonging to an iPhone.

b. Apple maintains the following records and information for iCloud accounts:

i. *Subscriber and billing information.* When a user registers an Apple device with an iCloud account, Apple collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and email addresses. Apple also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for some subscribers, Apple maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

ii. *Device information and settings*. Apple maintains information about the devices associated with an Apple ID and the data underlying account activity. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers for the device, such as the Integrated Circuit Card ID ("ICCID") number, which is the serial number on the device's SIM card, the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's device is captured when iTunes is used on that device to play content associated with an Apple ID. Information about a user's device settings may be captured and stored on iCloud. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

iii. *IP records.* Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as the iTunes Store and the App Store, iCloud, the Game Center, and the My Apple ID and iForgot pages on Apple's website.

iv. *Purchase records.* Apple maintains records reflecting a user's purchases from the App Store and iTunes Store.

v. *Address book.* Apple allows subscribers to maintain the equivalent of an address book on Apple devices, comprising telephone numbers, email addresses, and other contact information. That information may be backed up to a user's iCloud account.

vi. *Call history and voicemails*. Apple maintains records reflecting telephone call history and connectivity logs for Apple's native video call application, FaceTime. That information may be backed up to a user's iCloud account. Apple also allows iCloud subscribers to automatically backup voicemails and transcripts of those voicemails, which Apple calls "visual voicemail," to a subscriber's iCloud account.

vii. *Text message contents.* In general, text messages, Short Message Service ("SMS") messages, Multimedia Messaging Service ("MMS") messages, and iMessages sent to or from a subscriber's account are backed up to the iCloud unless and until the subscriber deletes the messages. If the subscriber does not delete messages, they can remain on the iCloud indefinitely. Even if the subscriber deletes messages off of an electronic device, they may continue to be available on the iCloud for a certain period of time.

viii. *Email contents*. In general, an iCloud account subscriber may elect to store and maintain email content on an iCloud account by linking one or more email accounts to Apple devices. When a subscriber links an email account, any email (which can include attachments such as documents, images, and videos) sent to or from that email account, or stored in draft form in

the account, is maintained on Apple's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Apple's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Apple's servers for a certain period of time. Additionally, to the extent a subscriber maintains an iCloud Mail account, iCloud enables a user to access Apple-provided email accounts, and email stored in those accounts are maintained by Apple.

ix. *Photos and videos.* In general, an iCloud account subscriber may elect to store and maintain photographs and videos on an iCloud account. Such photos may include pictures taken by devices linked to the iCloud account, pictures sent to those devices electronically, pictures downloaded onto those devices, and images created by device users who take a "screenshot" of whatever email, document, text message, or other record is displayed on the device screen. Any photograph or video stored in the account is maintained on Apple's servers unless and until the subscriber deletes the photograph or video. If the subscriber does not delete the photograph or video, it can remain on Apple's servers indefinitely. Even if the subscriber deletes a photograph or video, it may continue to be available on Apple's servers for a certain period of time. Additionally, if a subscriber uses iCloud Photo Library and My Photo Stream, which can be used to store and manage images and videos, or iCloud Photo Sharing, which allows users to share images and videos with other Apple subscribers, photographs and videos stored in those platforms are also maintained in a subscriber's iCloud account. Apple also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are stored on an iCloud account. This metadata includes what is known as exchangeable

image file format (or "Exif") data, and can include GPS location information for where a photo or video was taken.

x. *Documents.* An iCloud account subscriber may elect to store and maintain documents on an iCloud account by saving documents on an iPhone to the iCloud or by using the service iCloud Drive, which can be used to store documents to the iCloud. Additionally, iWork Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations.

xi. *Web history, search history, and bookmarks.* Apple maintains search and web browsing activity from Safari, Apple's proprietary web browser, as well as bookmarks used to save particular website addresses. iCloud account subscribers may also use iCloud Tabs, which enables iCloud to store and synchronize webpages opened in Safari web browsers on multiple devices, and iCloud Keychain, which enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

xii. *Third-party application data.* Records and data associated with third-party apps may also be stored on iCloud. For example, the iOS app WhatsApp, an encrypted instant messaging and calling service, can be configured to regularly backup a user's instant messages on iCloud.

xiii. *Location data*. Apple maintains recent location data, collected periodically, from mobile devices. For example, Apple collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location. The Apple application Find My iPhone, which enables owners of Apple devices to remotely identify and track

the location of devices, allows for location reporting, which allows Apple to periodically store and use a device's most recent location data in connection with an iCloud account.

xiv. *iOS Device Backups.* Apple allows iPhone users to back up the contents of their devices, including messages, web history, and preferences, to an iCloud account.

D. Jurisdiction and Authority to Issue Warrant

6. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Providers, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

7. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

8. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

A. Probable Cause Regarding the Commission of the Subject Offenses

9. I respectfully submit that probable cause exists to believe that BRUCE GARELICK, RAYMOND CORRAL, and PATRICK ORLANDO, among other individuals identified below,[1] have committed the Subject Offenses and/or that their email or iCloud storage accounts will contain evidence of the commission of the Subject Offenses.

Background

10. The FBI and the United States Attorney's Office for the Southern District of New York are investigating an insider trading scheme in securities of Digital World Acquisition Corporation ("DWAC"), a special purpose acquisition company ("SPAC")[2], the shares of which were publicly traded on the Nasdaq stock market beginning on or about September 3, 2021. On or about October 20, 2021, DWAC and Trump Media & Technology Group ("Trump Media"), a media and technology company founded in February 2021 by former United States President Donald J. Trump, announced that they had entered into a definitive merger agreement that would combine the two entities, allowing Trump Media to become a publicly-traded company. The investigation relates to disclosures in public filings by DWAC, as well as trading in DWAC stock in September and October 2021 based on material non-public information about its planned merger with Trump Media. As set forth below, there is probable cause to believe that ORLANDO, the chief executive officer of DWAC, made false statements in filings with the SEC by falsely stating that DWAC

[1] The term "Target Subjects" refers to Patrick Orlando, Bruce Garelick, Michael Shvartsman, Gerald Shvartsman, Raymond Corral, Anton Postolnikov, Adrian Lopez Torres, Javier Lopez Lopez, Eric Hannelius, and Allen Beyer.

[2] A special purpose acquisition company, also known as a "blank check company," is a publicly traded company created for the purpose of acquiring or merging with an existing private company, thus making it public without going through the traditional initial public offering process.

was not in negotiations with any SPAC target, even though DWAC was in negotiations with Trump Media and other entities at the time. Additionally, there is probable cause to believe that GARELICK, a DWAC director, CORRAL, and other individuals who appear to be affiliated with or known to GARELICK, purchased DWAC stock after learning non-public information about its planned merger with Trump Media, and sold the stock shortly after the merger was announced.

11. Based on my review of publicly available information, including but not limited to my review of filings made with the SEC, as well as documents produced by DWAC to the SEC, I have learned, among other things, the following about the business combination between DWAC and Trump Media:

a. On or about December 11, 2020, DWAC was formed in Delaware, and on or about February 8, 2021, Trump Media was formed in Delaware.

b. According to the *New York Times*, based on a confidential investor deck apparently reviewed by the publication, in or around March 2021, if not earlier, ORLANDO, who had previously launched SPACs, began discussions with former President Trump about taking Trump Media public through a SPAC.[3] Additionally, according to the *New York Times*, in April 2021 there was a video conference call among representatives of Trump Media, ORLANDO, and another individual who later became a board member of DWAC.[4]

c. On or about May 26, 2021, DWAC filed a Form S-1 registration statement with the SEC. The Form S-1 stated that DWAC was "a newly organized blank check company formed for the purpose of effecting a merger, capital stock exchange, asset acquisition, stock purchase,

[3] These facts have not yet been independently verified by the Government.

[4] These facts have not yet been independently verified by the Government. According to the article, a representative of Trump Media confirmed the call to the *New York Times* but said it was "strictly discussions between Trump Media and Benessere Capital Acquisitions," another SPAC that Orlando had previously run.

reorganization or similar business combination with one or more businesses." The Form S-1 also stated that DWAC had "not selected any specific business combination target and [had] not, nor [had] anyone on [its] behalf, initiated any substantive discussions, directly or indirectly, with any business combination target." ORLANDO, who was identified as the CEO and Chairman of DWAC, signed the registration statement. Although the Form S-1 identified director nominees, Bruce Garelick was not identified.

d. On or about July 8, 2021, DWAC filed an amended Form S-1 registration statement with the SEC, identifying GARELICK as a director nominee. According to the Form S-1, GARELICK is a "venture capitalist/entrepreneur/c-level executive and disruptive technology investing enthusiast" who currently serves as the chief strategy office of Rocket One Capital. As with the May 26 filing, the amended Form S-1 filing stated that DWAC had "not selected any specific business combination target" and had not "engaged in any substantive discussions, directly or indirectly, with any business combination target." DWAC filed additional amended Form S-1 registration statements on July 26, 2021, August 10, 2021, August 20, 2021, August 30, 2021, and August 31, 2021, which contained the same statement that DWAC had not selected a specific business combination target or engaged in substantive discussions with any target. Under SEC rules, a SPAC may not identify a specific target company prior to the closing of its initial public offering. The amended registration statement was signed by ORLANDO.

e. According to reporting in the *New York Times*, "[b]y the summer [of 2021], people affiliated with Trump Media were signaling in conversations with Wall Street financiers that they were nearing a deal to merge with a SPAC."[5]

[5] These facts have not yet been independently verified by the Government, and it is not clear whether DWAC was the special purpose acquisition vehicle referenced by people affiliated

f. On or about September 2, 2021, DWAC filed a Form 8-A registering securities with the SEC. On the same day, DWAC announced in a press release that it priced its initial public offering of $250 million, consisting of 25,000,000 units,[6] at $10.00 per unit, and that the units would be listed on the Nasdaq stock exchange the following day. The announcement stated that EF Hutton, a division of Benchmark Investments, LLC, was acting as sole book running manager for the offering, which means that if an individual wanted to purchase shares from the initial public offering at the offering's price—in other words, not on the public, secondary market—the shares had to be purchased through EF Hutton.

g. On or about September 2, 2021, GARELICK officially became a director of DWAC. As a director, GARELICK was subject to DWAC's Code of Ethics, which required, among other things, that he maintain the confidentiality of information entrusted to him by DWAC. The Code of Ethics also provided that "[e]mployees, officers and directors must not trade in securities of a company while in possession of material non-public information regarding that company," and that it is "illegal to 'tip' or pass on inside information to any other person who might make an investment decision based on that information or pass the information to third parties." The Code of Ethics stated that DWAC "has an Insider Trading Policy, which sets forth obligations in respect of trading in the Company's securities." Based on my conversations with SEC attorneys, I understand that DWAC has represented through counsel that a separate "Insider Trading Policy" does not yet exist.

---

with Trump Media. In particular, it is possible that these discussions related to Benessere Corporation, which, as noted, is another SPAC associated with Orlando.

[6] A "unit" consists of one share of the company's Class A common stock and one half of one redeemable warrant. Each warrant entitled the holder thereof to purchase one share of Class A common stock at a price of $11.50 per share.

h. On or about September 3, 2021, DWAC started trading publicly on the Nasdaq stock exchange.

i. On or about September 13, 2021, DWAC signed a confidentiality agreement (the "Confidentiality Agreement") with Trump Media Group Corp., noting that the parties were engaging in discussions about a possible business combination transaction and agreeing not to disclose any information regarding a possible transaction between the parties. In the Confidentiality Agreement, Trump Media Group Corp. "acknowledge[d] and agree[d] that some of the Confidential Information of DWAC and Transaction Information may be considered 'material non-public information' for purposes of the federal securities laws."

j. On or about September 14, 2021, and September 17, 2021, DWAC prepared a draft letter of intent with Trump Media Group Corp.[7] The letter of intent contains a provision regarding exclusivity, stating in sum and substance that neither party would enter into discussions, negotiations, or transactions with any other company or investor for a period of thirty days. It also stated that Trump Media Group Corp. "acknowledge[d] and agree[d] that some of the confidential information of [DWAC] (including [the letter of intent]) may be considered 'material non-public information' for purposes of the federal securities laws."

k. On or about September 21, 2021, starting at approximately 12:32 p.m., DWAC held a meeting of its board of directors over Zoom. Meeting minutes produced by DWAC show that GARELICK attended the meeting. According to those minutes, "[m]anagement introduced potential initial pipeline of targets," including Trump Media and several other companies. The minutes also stated that the "[c]onsensus of the board [was] to follow up/negotiate and execute

[7] Based on the materials provided by DWAC, it is unclear on what day the draft letter of intent was sent to Trump Media. The letter of intent purports to have been countersigned by former President Trump on September 22, 2021.

LOIs [letters of intent] with TMG [Trump Media], Global Oculus/Bittrex, and Wag! so that we may conduct deeper due diligence."[8]

l. On or about September 22, 2021, ORLANDO sent an update to the board of directors through WhatsApp regarding each of the potential acquisition targets. With respect to Trump Media, ORLANDO wrote: "[W]e had a great meeting and are have [sic] a follow up session very soon, we have gotten great traction on lowering the Enterprise Value of the target but are getting pushback on the flexibility to be unilaterally exclusive." ORLANDO asked the other directors whether they would agree to 30-day exclusivity with Trump Media. The directors responded that they were in favor of entering into an exclusivity period with Trump Media and GARELICK wrote, "I am enthusiastically in favor to advance with TMG [Trump Media] under the stated terms."

m. On or about September 27, 2021, according to press reports, ORLANDO went to Mar-a-Lago to meet with former President Trump and sign a letter of intent. As noted, the letter of intent, which is dated September 22, 2021, included an exclusivity clause providing that neither DWAC nor Trump Media would enter into discussions, negotiations, or transactions with any other company or investor for a period of thirty days.

n. On or about September 27, 2021, DWAC issued a press release and filed a Form 8-K announcing that its units could be split and traded separately starting on September 30, 2021. On or about September 30, 2021, DWAC units were split, and the shares of Class A common stock

[8] On or about September 20, 2021, DWAC and Global Oculus signed a non-binding letter of intent restricting Global Oculus's, but not DWAC's, ability to negotiate other business combination transactions. Two days later, as discussed herein, DWAC signed an exclusive letter of intent with Trump Media Group Corp.

and warrants started trading separately on the Nasdaq under the symbols "DWAC" and "DWACW," respectively.

o. On or about September 29, 2021, ORLANDO messaged the board of directors, including GARELICK, on the encrypted messaging application WhatsApp and wrote, in pertinent part, "We have a few updates and due diligence is kicking into high gear. TMG [Trump Media] wants to close on October 14th."

p. On or about October 19, 2021, from approximately 9:00 p.m. to 9:50 p.m., DWAC held a meeting of its board of directors over Zoom. Meeting minutes produced by DWAC show that GARELICK attended the meeting. According to those minutes, at the meeting the directors discussed whether to go ahead with the definitive agreement with Trump Media, and all directors voted in favor of signing the agreement. The minutes also indicate that the following day at 4 p.m. was the "[s]cheduled time to sign the definitive agreement" with Trump Media. The minutes further note that resolutions would be sent to board members via WhatsApp "to confirm unanimous decision to proceed with the signing of the definitive agreement."

q. On or about October 20, 2021, DWAC's share price closed at $9.96 with a total volume of 697,900.

r. According to the *New York Times*, on or about October 20, 2021, ORLANDO went to Mar-a-Lago where he met with former President Trump and they signed the deal.[9]

s. On or about October 20, 2021, at approximately 8:16 p.m., Liz Harrington, a spokesperson for former President Trump, posted a press release to Twitter announcing the merger of DWAC and Trump Media. The press release stated that Trump Media and DWAC had entered into a "definitive merger agreement, providing for a business combination that w[ould] result in

[9] These facts have not yet been independently verified by the Government.

[Trump Media] becoming a publicly listed company[.]" The release stated that the transaction valued Trump Media at as much as $1.7 billion. The release included a quote from former President Trump, who was identified as Chairman of Trump Media. The following day, DWAC filed a Form 8K related to the merger, which attached the October 20, 2021 press release announcing the business combination between DWAC and Trump Media.

t. Prior to the announcement of the business combination between DWAC and Trump Media, shares and units of DWAC were priced at approximately $10 per unit or share, and warrants were priced at approximately $0.50 per warrant. Following the public announcement, DWAC shares peaked at approximately $175 per share, warrants peaked at approximately $79 per warrant, and units peaked at approximately $142 per unit. As of February 9, 2022, DWAC shares are trading at approximately $82 per share, DWAC warrants are trading at approximately $27 per warrant, and DWAC units are trading at approximately $95 per unit.

12. Based on my review of public sources and news articles, it does not appear that there was any public reporting about a merger between DWAC and Trump Media until the day the business combination was announced: October 20, 2021, in the evening.

Trades by GARELICK

13. Based on my review of brokerage records, telephone records, and records from DWAC obtained via subpoena or produced by the SEC, as well as from my review of public sources, there is probable cause to believe that GARELICK traded in DWAC stock on the basis of material non-public information. Specifically, I have learned the following:

a. As noted above, on or about July 8, 2021, GARELICK became a director nominee of DWAC, and on or about September 2, 2021, he became an official director of DWAC. Prior to that period, it appears that DWAC was in discussions with Trump Media to enter into a business

combination. I have reviewed telephone records for the cellphone number [redacted]5950, which is subscribed to in the name of BRUCE GARELICK (the "Garelick Cellphone Number"). Based on my review of records for the Garelick Cellphone Number, I have learned that on or about September 1 and September 2, 2021, GARELICK and ORLANDO, who was using the cellphone number [redacted]1513 (the "Orlando Cellphone Number") had several telephone calls. Accordingly, there is reason to believe that because of his board role, and conversations with ORLANDO, GARELICK had non-public information about DWAC's potential merger with Trump Media on or before September 2, 2021. On or about September 3, 2021, the first day DWAC units were trading on the Nasdaq, using an account at Fidelity in his name, GARELICK purchased a total of 610 units of DWAC at prices ranging from $10.01 to $10.02 per unit.[10] On September 10, 2021, GARELICK purchased 300 units of DWAC at $10.02 per share.

b. As discussed above, it appears that on or about September 14 and September 17, 2021, DWAC prepared and possibly sent draft letters of intent to Trump Media Group Corp. On or about September 17, 2021, using his Fidelity account, GARELICK purchased a total of 410 units of DWAC at $10.05 per unit. On or about September 20, 2021, using his Fidelity account, GARELICK purchased 900 units of DWAC at prices ranging from $10.03 to $10.04 per unit.

c. As discussed above, on September 21, 2021, at approximately 12:32 p.m., DWAC held a board meeting, at which GARELICK was present, and discussed potential acquisition targets, including Trump Media. On or about September 21, 2021, shortly before the start of the board meeting, using his Fidelity account, GAERLICK purchased a total of 1,800 units of DWAC

[10] Because September 3, 2021, was the first day of trading, it is possible Garelick purchased DWAC units because he was excited about the business and not because he knew of material non-public information. Garelick, however, did not buy units from EF Hutton, the sole book running manager for the initial offering, but instead through his Fidelity account on the secondary market.

at approximately $10.05 per unit. As discussed above, on September 22, 2021, ORLANDO provided an update via WhatsApp to the board of directors about a deal with Trump Media progressing. On or about September 23, 2021, using the same account, GARELICK purchased a total of 1,300 units of DWAC at approximately $10.07 per unit.

d. On or about October 21, 2021, after the merger with Trump Media was announced, GARELICK sold all of his shares of DWAC in his Fidelity account for share prices ranging from $14.30 to $19.23.[11] GARELICK also sold all the DWAC warrants in his Fidelity account. In total, GARELICK made approximately $49,702 in profit on these sales.

e. From my training and experience, I have learned that federal securities regulations require certain individuals, such as officers and directors, to report purchases, sales, and holdings of their company's securities to the SEC by filing Forms 3 and 4. Company insiders, such as officers and directors, must file a Form 3 to initially disclose their ownership of the company's securities within ten days of becoming an insider. When an insider executes a transaction, he or she must file a Form 4 within two days, which discloses the transaction to the public. From my review of SEC filings, I have learned that notwithstanding the fact that GARELICK was a director of DWAC during part of the period when he was trading, he did not file a Form 3 or Form 4 for any of his purchases or sales of DWAC units or shares.

14. Based on my review of brokerage records, telephone records, and records from DWAC obtained via subpoena or produced by the SEC, as well as from my review of public sources, there is probable cause to believe that GARELICK told one or more other individuals non-public information about DWAC's planned business combination with Trump Media, and that those

[11] After DWAC allowed its shareholders to split units into shares and warrants, GARELICK requested that Fidelity divide all his units into shares and warrants of DWAC. Fidelity did so before GARELICK sold his holdings in DWAC.

individuals traded on the basis of that information, and in some cases tipped other individuals who traded in the stock. Each of the individuals identified below purchased units, shares, and/or warrants of DWAC while it was publicly known as a blank check company (in other words, it did not have a planned combination target), before there was any news about a merger with Trump Media, and then sold those units, shared, or warrants right after the merger announcement. Specifically, I have learned the following:

Trades by Rocket One Capital (MICHAEL SHVARTSMAN)

a. GARELICK is chief strategy officer of Rocket One Capital, as noted above. Rocket One Capital is a venture capital firm in Miami, Florida, headed by MICHAEL SHVARTSMAN. Based on my review of telephone records, it appears that GARELICK, using the Garelick Cellphone Number, and MICHAEL SHVARTSMAN communicate regularly by telephone and text message.

b. On or about August 30, 2021, GARELICK, using the Garelick Cellphone Number, and MICHAEL SHVARTSMAN exchanged at least four telephone calls. On the same day, MICHAEL SHVARTSMAN opened a brokerage account in the name of Rocket One Capital, LLC. On or about September 1 and September 2, 2021, MICHAEL SHVARTSMAN and GARELICK, using the Garelick Cellphone Number, exchanged multiple telephone calls. On or about September 2, 2021, the Rocket One Capital account was funded and on September 3, 2021, the first day of trading for DWAC units, Rocket One Capital purchased 14,500 units of DWAC.

c. As noted above, by on or about September 27, 2021, if not earlier, DWAC and Trump Media had signed an exclusive letter of intent, and on or about September 29, 2021, ORLANDO messaged the board of directors, including GARELICK, “due diligence is kicking into high gear” on the Trump Media merger. On or about October 1, October 4, and October 5,

MICHAEL SHVARTSMAN and GARELICK exchanged multiple telephone calls. On or about October 1, 2021, Rocket One Capital purchased approximately 227,915 DWAC warrants; on or about October 4, 2021, Rocket One Capital purchased approximately 1,641,731 DWAC warrants; and on or about October 5, 2021, Rocket One Capital purchased approximately 130,354 warrants.

d. On or about October 21 and 22, 2021, Rocket One Capital sold off its shares in DWAC for approximately $18.4 million in realized profit. The Rocket One Capital account was not used for any other trading.

Trades by GERALD SHVARTSMAN

e. Based on my review of publicly available information, it appears that GERALD SHVARTSMAN is the brother of MICHAEL SHVARTSMAN. From telephone records, it appears that GERALD SHVARTSMAN uses the telephone number [redacted]3470 (the "Gerald Shvartsman Number") to speak with MICHAEL SHVARTSMAN nearly daily, and sometimes multiple times per day. GERALD SHVARTSMAN appears to be the owner of Source Furniture in Miami, Florida, which appears to be a furniture supply store.

f. On or about August 5, 2021, GERALD SHVARTSMAN opened a brokerage account with Benchmark Investments which, as noted above, was the sole book running manager for DWAC's initial public offering. On or about August 11, 2021, GERALD SHVARTSMAN wired funds into the account.

g. On or about September 3, 2021, MICHAEL SHVARTSMAN and GERALD SHVARTSMAN exchanged telephone calls at approximately 9:09 a.m., 9:20 a.m., 10:52 a.m., 11:03 a.m., 11:13 a.m., and 5:05 p.m. On or about September 3, 2021, GERALD SHVARTSMAN purchased 10,800 units of DWAC at approximately 1:22 p.m.

h. Between on or about October 7 and October 18, 2021, GERALD SHVARTSMAN purchased 400,000 warrants of DWAC.

i. On or about October 21 and 22, 2021, GERALD SHVARTSMAN sold all his shares of DWAC for a profit of $5.1 million.

Trades by RAY CORRAL

j. Based on my review of public sources, I have learned that RAY CORRAL is associated with MICHAEL SHVARTSMAN, and it appears they are friends. For example, I have reviewed an image available online of MICHAEL SHVARTSMAN and RAY CORRAL together at what appears to be a social event at The Deck at Island Gardens, a super yacht marina, in February 2016. From my review of telephone records, including records of the telephone number [redacted]5944 subscribed to Ray Corral (the "Corral Cellphone Number"), it appears that MICHAEL SHVARTSMAN and CORRAL communicate regularly by telephone. Additionally, it appears from telephone records that CORRAL knows GARELICK, because they appear to have spoken by telephone on or about June 30, July 1, July 9, July 16, and October 21, 2021. It also appears that CORRAL knows GERALD SHVARTSMAN because, according to telephone records, they communicated on July 2, 2021.

k. On or about August 4, 2021, CORRAL opened an account at Benchmark Investments, and on or about August 10, 2021, he wired funds into the account.

l. On or about September 3, 2021, at approximately 9:11 a.m., MICHAEL SHVARTSMAN called CORRAL, and the two spoke for several minutes. On or about the same day, September 3, 2021, at approximately 1:22 p.m., CORRAL purchased 10,740 units of DWAC. MICHAEL SHVARTSMAN and CORRAL spoke several more times in September and early October 2021.

m. On or about October 21, 2021, CORRAL called MICHAEL SHVARTSMAN. CORRAL again called MICHAEL SHVARTSMAN on or about October 22, 2021. On or about October 21 and October 22, 2021, CORRAL sold all his holdings of DWAC for a profit of $268,342.

Trades by APLC Investments LLC (Anton Postolnikov)

n. Based on my review of public sources and bank records, I have learned that Anton Postolnikov is a Russian citizen living in Miami, Florida, who appears to be the owner of APLC Investments LLC. Based on my review of telephone records, it appears that Postolnikov knows ORLANDO, GARELICK, MICHAEL SHVARTSMAN, GERALD SHVARTSMAN, and RAYMOND CORRAL, and communicated with ORLANDO and GERALD SHVARTSMAN regularly between September and November 2021.

o. On or about August 11, 2021, APLC Investments LLC opened an account at Benchmark Investments and wired funds into the account on or about August 12, 2021. The signatory on the APLC Investments account is Postolnikov.

p. On or about September 3, 2021, Postolnikov purchased a total of 4,75,110 units of DWAC. On or about September 8, 2021, Postolnikov purchased 5,000 units of DWAC. On or about October 6, 2021, Postolnikov purchased 510 units of DWAC. On or about October 11, 2021, Postolnikov purchased 20,800 units of DWAC. On or about October 12, 2021, Postolnikov purchased 100,000 warrants of DWAC. On or about October 18, 2021, Postolnikov purchased 100,000 warrants of DWAC. On or about October 19, 2021, Postolnikov purchased 74,517 warrants of DWAC. On or about October 20, 2021, Postolnikov purchased 175,000 warrants of DWAC.

q. During the period in which Postolnikov purchased units and warrants of DWAC, he communicated by telephone with ORLANDO and GERALD SHVARTSMAN.

r. From on or about October 21 through on or about October 28, 2021, Postolnikov liquidated substantially all his DWAC holdings for a profit of approximately $22.8 million.

Trades by Eric Hannelius

s. Based on my review of public sources, I have learned that MICHAEL SHVARTSMAN is a partner in multiple businesses with Eric Hannelius. Based on my review of telephone records between MICHAEL SHVARTSMAN and Hannelius, it appears they speak at least once per week. Additionally, from my review of telephone records, it appears that GARELICK and Hannelius communicate from time to time by telephone and text message.

t. On or about September 12, 2021, MICHAEL SHVARTSMAN and Hannelius spoke by telephone. On or about September 13, 2021, Hannelius purchased 500 DWAC units.

u. On or about October 4, October 5, and October 6, MICHAEL SHVARTSMAN and Hannelius spoke by telephone. Between in or about October 6 and in or about October 7, 2021, Hannelius bought 11,300 DWAC warrants.

v. On or about October 21, 2021, Hannelius sold all his holdings in DWAC for a total net profit of $168,206.

Trades by Adrian Lopez Torres and Javier Lopez Lopez

w. Based on my review of publicly available sources and brokerage records, it appears that Adrian Lopez Torres ("Torres") was an employee at Source Furniture which, as noted above, is owned by GERALD SHVARTSMAN.

x. On or about October 19, 2021, one day before the public announcement of the merger between DWAC and Trump Media, Torres placed an order to purchase DWAC warrants, and on or about October 20, 2021, in the morning, Torres purchased 100,000 DWAC warrants.

y. On or about October 19, 2021, Javier Lopez Lopez ("Lopez"), the father of Torres according to broker records, placed an order to purchase DWAC warrants, and on or about October 20, 2021, in the morning, Lopez purchased 40,000. Based on my review of brokerage records, it appears that Lopez is a technician at a dialysis clinic.

z. On or about October 21, 2021, Torres sold the DWAC warrants for a profit of $404.411. On or about October 22, 2021, Lopez sold his DWAC warrants for a profit of $1.58 million.

15. Based on the foregoing, there is probable cause to believe that ORLANDO made false statements to the SEC in DWAC's filings by falsely representing that DWAC was not negotiating with a SPAC target. Additionally, there is probable cause to believe that GARELICK knew of material non-public information about DWAC's planned merger with Trump Media, that he traded on the basis of that information. There is also probable cause to believe that ORLANDO, GARELICK, and others provided that material non-public information to friends and/or associates, including MICHAEL SHVARTSMAN, GERALD SHVARTSMAN, and RAY CORRAL, among others, who then traded on the basis of that information and passed it to their associates, all in violation of the Subject Offenses.

B. Probable Cause Regarding the Subject Accounts

16. On or about December 29, 2021, the Honorable Marcia M. Henry of the United States District Court for the Eastern District of New York signed a warrant authorizing the search and seizure of a cellphone in the possession of GARELICK. On or about December 31, 2021, law enforcement agents surreptitiously executed the warrant while GARELICK was reentering the

United States at John F. Kennedy Airport upon his return from international travel. Specifically, law enforcement agents seized, reviewed, and returned an iPhone 11 Pro Max registered with the Garelick Cellphone Number. Due to the covert nature of the search and this investigation more broadly, law enforcement agents were unable to obtain an entire forensic image of GARELICK's cellphone. Instead, an agent reviewed certain contents of the phone manually and took screenshots (the "Garelick Cellphone Screenshots") of selected information, including certain text messages, calendar entries, and contact information determined to be responsive to the warrant. Based on my review of the Garelick Cellphone Screenshots, I have learned the following:

a. On or about June 21, 2021, GARELICK, using the Garelick Cellphone Number, sent MICHAEL SHVARTSMAN a text message that stated, "FYI – Patrick Orlando call tomorrow at 3pm. Please let me know Ojus and your brothers email addresses. . . . so I can include them on the invites."

b. On or about June 23, 2021, at 10:2 a.m., an individual saved in GARELICK's phone as "Allen Beyer"[12] sent a text message to GARELICK and MICHAEL SHVARTSMAN in which he wrote the following:

> Thoughts on TMG:
> DT hyped up his "From the Desk of Donald Trump" social platform and it TANKED. Was an embarrassment.
>
> A President cannot use his public political position for his own personal financial gains.
>
> (Consider: he may run for president but never win. If Desantis runs on another ticket he would destroy him. This would allow DT to do whatever he wants and be the best case scenario for this "social media platform.")
>
> Next thing to consider: Is there even a social media platform? Do they have tech plans/ If they do, what are they and can it be successful out of the gate

[12] According to a publicly available LinkedIn account for Beyer, he is the Vice President for Strategic Partnerships and a "Venture Partner" at Rocket One Capital.

> in terms of adoption by other key political figures/ social media figures? If it's just an app with Forever Trumpers – this can easily be a bust . . many Americans, even staunch conservative political figures, may not create accounts for obvious-risks to reputation/ not sure Republican Party is going to want to get in bed again with DT unless it's absolutely necessary (thinking for themselves/ party progression)
>
> More thoughts: Michael, do you think we can actually help with tech development (would trump decision- makers go for it?) / ability to reuse components of Joblio
>
> Can you trust this "let's make it happen at all costs-type" dude (forgot his name) to do this the right way and would you ever be associated with this as a "founder" or anything in case it goes up in literal flames?
>
> Best chance is if he becomes just kinda a "behind the scenes/puppet master" of politics and encourages people to use his platform that way . . . if he runs it will be much tougher.
>
> Another thing. If he uses AWS, Google, all those hosting platforms, he runs the risk of them deplatforming him.
>
> Also he's been hyping up Parler and all those other small ones for so long now . . . same w DJTJ and Eric. What's gonna differentiate from those?

c. According to GARELICK's calendar on his cellphone, on or about June 28, 2021, there was a call between "DWAC/Rocket One Capital," and then later that day a call between "Mike/Bruce to discuss DWAC terms."

d. On or about June 30, 2021, at 9:53 a.m., Beyer texted a screenshot of a news alert to GARELICK and MICHAEL SHVARTSMAN, which included the headline: "The Trump Organization and its CFO are expected to be charged with tax-related crimes by the Manhattan DA Thursday, say people familiar with the matter." Below that screenshot, Beyer wrote, "Fresh off the Wall Street Journal. Would something like this impact their ability to even take a co public right now." GARELICK responded, "Yes. There is certainly risk the SPAC does not get the Trump media group for a variety of reasons However, we have downside protection from the

structure of the investment." Beyer responded, "Buy now pay later[.] You guys realize what this actually does right? It Puts the Street Dealer Out of Business."

e. On or about July 1, 2021, at 10:41 a.m., GARELICK sent a text message to a number stored in his phone as "Ray Corral." The contact card for "Ray Corral" in GARELICK's cellphone lists the Corral Cellphone Number and identifies him as a "friend of Mike S," which appears to be a reference to MICHAEL SHVARTSMAN, and "Joblio prospective investor-Feb 2021." In the text message, GARELICK wrote: "Ray. It's Bruce Garelick. Do you still want to speak regarding the SPAC deal? If so, please let me know a good time to call you today." In response, CORRAL stated, "Yes calling u in 30 / Call please thank you / Ray@mosaicist.com." In other words, it appears that CORRAL was providing his email address to GARELICK for further communication.

f. On or about July 9, 2021, at 10:26 a.m., CORRAL wrote: "Bruce good morning / When u going public with the spac / Trump." GARELICK responded, "I think the IPO is schedule for next week."

g. According to GARELICK's cellphone calendar, he had an entry on July 30, 2021, to "email DWAC investors with $5 options + Arcadian schedule." The entry was saved under the calendar for bruce.m45@gmail.com.

h. On or about August 31, 2021, MICHAEL SHVARTSMAN wrote, "I'll call you back." Later that day, GARELICK said "Just called u back. Grabbing din with my girl now. Urgent? Talk later?" MICHAEL SHVARTSMAN responded, "Nope call later."

i. On or about September 1, 2021, GARELICK sent a text message to the Orlando Cellphone Number, which is stored in GARELICK's cellphone as "Patrick O," and which based on the conversation that follows, GARELICK understood to be ORLANDO. GARELICK stated,

"Patrick – it's Bruce Garelick at Rocket One. Congrats on the IPO date becoming official! Let's briefly catch up when you get a minute."

j. On or about September 2, 2021, at 9:18 a.m., GARELICK wrote, "I spoke to Patrick Orlando. Not urgent. We can catch up later." On or about October 1, 2021, GARELICK sent MICHAEL SHVARTSMAN a screenshot of what appears to be a Yahoo finance lookup of DWAC warrants' trading activity.

k. According to GARELICK's cellphone calendar, on September 21, 2021, there was a "DWAC Board of Directors Meeting" by Zoom.

l. According to GARELICK's cellphone calendar, on or about October 18, 2021, there was a DWAC board meeting by Zoom. On or about October 19, 2021, there was a "DWAC Board Meeting" by Zoom. On or about October 20, 2021, a "TMTG Financial Model Discussion" was scheduled to be held by Zoom.

17. Based on my review of brokerage records, telephone records, records produced by Apple and WhatsApp (currently owned by Meta), records produced by DWAC, the Garelick Cellphone Screenshots, and publicly available records, I submit that there is probable cause to believe that the Subject Accounts will contain evidence of the commission of the Subject Offenses. Specifically:

a. Subject Account-1 and Subject Account-2 are iCloud accounts registered to GARELICK. According to records from Apple, both accounts are registered with the Garelick Cellphone Number. Additionally, according to Apple records, both accounts have enabled iCloud backups of iOS devices, calendar backups, iCloud Drive, and contacts.[13] From my review of the

[13] Based on my review of the Garelick Cellphone Screenshots, it appears that iCloud backup for contacts and iOS devices was enabled, but no other features were set to be backed up

Garelick Cellphone Screenshots, I know that the Apple ID on GARELICK's cellphone listed the associated email addresses for both Subject Account-1 and Subject Account-2. As discussed above, GARELICK used text messages to communicate with MICHAEL SHVARTSMAN, Allen Beyer, ORLANDO, and CORRAL about DWAC, Trump Media, and other financial and investment-related matters. Additionally, from records provided to the SEC by DWAC, I know that GARELICK used WhatsApp to communicate with ORLANDO and other individuals about DWAC board meetings and votes. For example, on or about September 29, 2021, ORLANDO texted the DWAC directors on WhatsApp that "due diligence is kicking into high gear" and that Trump Media "wants to close on October 14th." As to GARELICK, such communications are evidence of the commission of the Subject Offenses because they will indicate what non-public information GARELICK had when he traded and/or told other individuals to buy DWAC units, shares, or warrants.[14] Therefore, based on my training, experience, and review of information provided publicly by Apple, records from GARELICK's cellphone with the Garelick Cellphone Number are likely to have been backed up to Subject Account-1 and Subject Account-2, and Subject Account-1 and Subject Account-2 are likely to contain records of the communications described above.

b. Subject Account-3 is an iCloud account registered to ORLANDO. According to records from Apple, the account is registered with the Orlando Cellphone Number. Additionally, according to Apple records, the account has enabled iCloud backups of iOS devices, calendar

---

to the iCloud. As noted above, records from Apple indicate additional records are being backed up to the iCloud.

[14] Based on my training and experience, WhatsApp records are typically backed up to an iCloud account with other text messages or chats, such as SMS. When law enforcement agents executed a search on GARELICK's cellphone, they were able to verify that GARELICK had a WhatsApp account on the cellphone, but they were unable to access the messages. At the time, WhatsApp did not appear to be backed up to the iCloud.

backups, photos backup, iCloud Drive, mail backup, messages backup, notes backup, and contacts. As described above, ORLANDO used the Orlando Cellphone Number to communicate with GARELICK about DWAC. Telephone records for the Orlando Cellphone Number also indicate that he communicated with Postolnikov, and therefore Subject Account-3 is likely to contain records of text messages or telephone calls with him. As discussed above, ORLANDO also used WhatsApp to communicate with members of the DWAC board about updates on the SPAC and board decisions or meetings. Additionally, as noted above, mail is backed up to Subject Account-3, and the primary email address registered to Subject Account-3 is patorlando1@gmail.com. According to information provided by DWAC, through counsel, to the SEC, ORLANDO may have used that email account to conduct business on behalf of DWAC, and therefore emails about DWAC are likely to have been backed up to Subject Account-3. From my training, experience, and review of information provided publicly by Apple, records from ORLANDO's cellphone with the Orlando Cellphone Number are likely to have been backed up to Subject Account-3, and therefore Subject Account-3 is likely to contain records of the communications described above.

c. Subject Account-4 is an iCloud account registered to GERALD SHVARTSMAN. According to records from Apple, the account is registered with the Gerald Shvartsman Number. Additionally, according to Apple records, the account has enabled iCloud backups of iOS devices, calendar backups, photos backup, iCloud Drive, mail backup, messages backup, notes backup, and contacts. From my review of the Garelick Cellphone Screenshots, I have learned that GARELICK has the Gerald Shvartsman Number saved in his phone under the name "Gerald Shvartsman" and has the note "Source Outdoor Furniture." As discussed above, it appears that GERALD SHVARTSMAN is the owner of or affiliated with Source Furniture in Florida. As discussed above, GERALD SHVARTSMAN used the Gerald Shvartsman Number to communicate with

MICHAEL SHVARTSMAN extensively, including on or about September 3, 2021, when GERALD SHVARTSMAN and MICHAEL SHVARTSMAN exchanged five telephone calls, and GERALD SHVARTSMAN purchased 10,800 units of DWAC. According to telephone records, the Gerald Shvartsman Number was also used to communicate with CORRAL, Postolnikov, and Adrian Lopez Torres. In particular, Torres, who was an employee at Source Furniture, purchased DWAC warrants on October 19, 2021, one day before the public announcement with Trump Media, and therefore it is likely that GERALD SHVARTSMAN was the source of the stock recommendation to Torres. Additionally, I have reviewed brokerage records for GERALD SHVARTSMAN, and the Gerald Shvartsman Number is listed as his contact telephone number. From my training and experience, it is common for an individual to receive texts or emails to the cellphone number they use to register a brokerage account, and therefore the Gerald Shvartsman Number likely received brokerage-related information. Finally, from my training, experience, and review of information provided publicly by Apple, records from GERALD SHVARTSMAN's cellphone with the Gerald Shvartsman Number are likely to have been backed up to Subject Account-4, and therefore Subject Account-4 is likely to contain records of the communications described above.

d. Subject Account-5 is an iCloud account registered to RAYMOND CORRAL. According to records from Apple, the account is registered with the cellphone number [redacted] 5944 (the "Corral Cellphone Number"). Additionally, according to Apple records, the account has enabled iCloud backups of iOS devices, calendar backups, photos backup, iCloud Drive, mail backup, messages backup, notes backup, and contacts. From my review of the Garelick Cellphone Screenshots, I know that CORRAL used text messages to communicate with GARELICK. For example, as quoted above, on July 1, 2021, GARELICK texted CORRAL, in relevant part, "Do

you still want to speak regarding the SPAC deal?" and CORRAL responded, "Yes calling u in 30." From my review of telephone records, it also appears that CORRAL used the Corral Cellphone Number to communicate about DWAC transactions. For instance, on September 3, 2021, CORRAL communicated with Michael Shvartsman and then later that day purchased 10,740 units of DWAC. On October 21, 2021, CORRAL used the Corral Cellphone Number to communicate with MICHAEL SHVARTSMAN and then on October 21 and October 22, 2021, sold all of his holdings of DWAC. Additionally, I have reviewed brokerage records for CORRAL, and the Corral Cellphone Number is listed as his contact telephone number. From my training and experience, it is common for an individual to receive texts or emails to the cellphone number they use to register a brokerage account, and therefore the Corral Cellphone Number likely received brokerage-related information. Finally, from my training, experience, and review of information provided publicly by Apple, records from CORRAL's cellphone with the Corral Cellphone Number are likely to have been backed up to Subject Account-5, and therefore Subject Account-5 is likely to contain records of the communications described above.

e. Subject Account-6 is an email account belonging to GARELICK that is hosted by Google. Based on my review of records produced by Fidelity, I have learned that Subject Account-6 was listed as GARELICK's contact email address, and was used by GARELICK to communicate with Fidelity about his account. From my training and experience, it is common for an individual to receive emails to the email address they use to register a brokerage account, including emails about the trading of stock and warrants, and therefore Subject Account-6 likely received brokerage-related information from Fidelity about GARELICK's trades of DWAC. Additionally, as noted above, GARELICK used email to communicate about DWAC, including with CORRAL,

and therefore there is reason to believe Subject Account-6 will contain communications about DWAC and transacting in its stock.

f. Subject Account-7 is an email account belonging to MICHAEL SHVARTSMAN that is hosted by Google. Based on my review of brokerage records, I have learned that the Rocket One Capital LLC brokerage account used to buy and sell units of DWAC was opened by MICHAEL SHVARTSMAN and registered with the email address for Subject Account-7. From my training and experience, it is common for an individual to receive emails to the email address they use to register a brokerage account, including emails about the trading of stock and warrants, and therefore Subject Account-7 likely received brokerage-related information about Rocket One Capital's trades of DWAC.

g. Subject Account-8 is an email account belonging to CORRAL that is hosted by Google. Subject Account-8 is listed as the contact email address for CORRAL in GARELICK's cellphone, and based on my review of the Garelick Cellphone Screenshots, discussed above, the address for Subject Account-8 was sent via text to GARELICK from CORRAL in connection with the conversation about discussing DWAC. Accordingly, there is reason to believe that CORRAL used Subject Account-8 to communicate with GARELICK about DWAC.

h. Based on my review of records provided by Apple and Meta, and from the execution of the search warrant on GARELICK's cellphone, I know that GARELICK, MICHAEL SHVARTSMAN, and CORRAL have and use smartphones with email capabilities. Specifically, GARELICK and CORRAL have iPhones and MICHAEL SHVARTSMAN has an Android device. As described above, GARELICK, MICHAEL SHVARTSMAN, and CORRAL communicated with each other by text messages – which appear to have been sent by their cellphones – about DWAC and other financial matters. Based on my training and experience, I

know that individuals who communicate via text messages also often communicate via email, particularly where the subjects use devices that contain both capabilities. In particular, individuals who engage in insider trading often use email to, among other things, communicate with co-conspirators; review, send, and comment on documents relevant to the execution of the fraud scheme; and coordinate in-person and virtual meetings. Accordingly, Subject Account-6, Subject Account-7, and Subject Account-8 are likely to contain evidence relating to DWAC and stock trading in the SPAC.

18. Based on my training and experience investigating other insider trading schemes, I know that email and iCloud accounts often contain the following types of evidence relating to the commission of the Subject Offenses:

a. Email and iCloud accounts typically contain identifying information that helps to verify the user of an account, as well as evidence of other accounts and, in the case of iCloud accounts, devices, belonging to the user. They may also contain passwords to access those accounts or devices.

b. Email and iCloud accounts typically contain evidence establishing the existence of a relationship between two or more people that are members of a conspiracy, or who may have tipped each other regarding non-public information about a security. Such information can include contact information, images, documents, and emails (and, in the case of iCloud accounts, text messages or messages from third-party applications that are backed up to the iCloud account) between or among the individuals. Such information is relevant to establishing the existence of a relationship between members of a conspiracy, their knowledge of each other's activities, and the fact that their relationship was one where they would engage in criminal activity together.

c. Email and iCloud accounts often contain documents relevant to the execution of a fraud scheme. Such documents often come in the form of transaction documents, such as brokerage statements, meeting minutes, and deal documents. Documents may also come in the form of emails, such as emails about a transaction or email confirmation about the execution of a trade.

d. Emails and iCloud accounts often contain records of web activity, web history, search history, browsing history, and bookmarks. Such records often contain evidence of an account user's then-existing mental state, and will also often contain evidence of an individual's plans, intentions, and/or knowledge about a course of criminal conduct.

e. Email and iCloud accounts may also contain evidence of location, including IP records, calendar invitations or entries, and photographs of locations. Such location information may establish that, for example, two or more members of a conspiracy were together at, around, or shortly before the time one member of a conspiracy traded in DWAC stock. Similarly, such location information may establish that the Target Subjects were at meetings when material non-public information was communicated.

f. Google and iCloud accounts may also contain backups of Android and Apple devices, which can include each of the types of data set forth above, including emails, text messages, documents, photos, and third-party application data. Accordingly, there is reason to believe that any device backup will contain evidence of the Subject Offenses.

g. Based on my training and experience, I know that a VoIP number can be associated with a Google account through the Google Voice service, and records from Google Voice can provide information about communications among co-conspirators. Additionally, from my

training and experience, I know that individuals involved in fraud will routinely use VoIP numbers to place telephone calls in a covert manner in order to avoid surveillance by law enforcement.

19. Temporal Limitation. This application seeks the production of emails from December 11, 2020, the date on which DWAC was formed, through the present. Because even recently stored device backups may include communications that occurred during the time period under investigation, the iCloud data is sought without date limitation. The materials to be seized from the Subject Accounts will be limited, to the extent they are dated, to those created, sent, received, modified, or deleted on or about December 11, 2020.

C. Evidence, Fruits and Instrumentalities

20. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Providers' servers associated with the Subject Accounts will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachments A and B to the proposed warrants.

21. In particular, I believe the Subject Accounts are likely to contain the following information:

a. Evidence sufficient to establish the user(s) of the Subject Accounts at times relevant to the Subject Offenses, including photographs, contact information, payment information, and other personally identifiable information;

b. Evidence of knowledge of the prohibition against insider trading in securities;

c. Evidence of knowledge of the required disclosures on SEC Form S-1 or other SEC filings related to SPAC transactions;

d. Evidence of the Target Subjects' knowledge or understanding that DWAC's disclosures on SEC Form S-1 were false or misleading;

e. Evidence relating to DWAC including, but not limited to, its business combination with Trump Media, Trump Media Group Corp., or other potential combination targets (or the lack thereof);

f. Evidence relating to the Target Subjects' knowledge of the fact that information about DWAC and/or Trump Media or Trump Media Group Corp. was confidential and/or non-public;

g. Evidence relating to the conveyance of material non-public information regarding DWAC, Trump Media, Trump Media Group Corp., or other potential combination targets (or the lack thereof);

h. Evidence relating to DWAC's selection of business combination target(s), including, but not limited to, the dates and substance of discussions or negotiations with combination targets, and public filings about DWAC's selection of a business combination target.

i. Evidence of the Target Subjects' ownership and control over brokerage accounts, and their history of trading securities;

j. Evidence relating to trading in units, warrants, or shares of DWAC;

k. Communications involving one or more of the Target Subjects, members of the board of directors of DWAC, or any other individual who traded in DWAC units, stock, or warrants;

l. Evidence of the existence of relationships between the Target Subjects, members of the board of directors of DWAC, or any other individual who traded in DWAC units, stock, or warrants[15];

[15] In light of *Dirks v. Securities and Exchange Commission*, 463 U.S. 646 (1983), and its progeny, for insider-trading related violations of Title 15, United States Code, Sections 78j(b) and

m. Evidence relating to Trump Media, including news about Trump Media;

n. Evidence reflecting the state of mind of (i) individuals involved in trading in the units, warrants, or shares of DWAC, and (ii) individuals possessing, or having access to, material non-public information regarding the business combination between DWAC and Trump Media;

o. Evidence of the receipt, transfer, disposition, or location of funds raised through the commission of the Subject Offenses;

p. Evidence of efforts to conceal the commission of the Subject Offenses and evade detection by law enforcement and/or regulatory agencies;

q. Evidence of the geographic location of the users of the Subject Accounts;

r. Evidence of passwords or other information needed to access the Subject Accounts or other accounts of the users of the Subject Accounts;

s. Evidence relating to other accounts, devices, or physical premises in which evidence of the commission of the Subject Offense may be found; and

t. Evidence concerning the identities of, and communications with, co-conspirators.

III. Review of the Information Obtained Pursuant to the Warrants

22. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of

---

78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5, the Government must in some instances prove that the tipper receives a "personal benefit" in exchange for the information he or she provides. One means by which the Government satisfies the requirement that the tipper receive some sort of benefit for the information he or she passes is by establishing that the insider provided information in a manner akin to "mak[ing] a gift of confidential information to a trading relative or friend," *id.* at 664; *see also id.* (noting that, when there is a gift of information to a relative or friend, "[t]he tip and trade resemble trading by the insider himself followed by a gift of the profits to the recipient"), which requires proof of the relationship between tipper and tippee. Accordingly, any information found in the Subject Accounts relating to the nature and history of the relationships between the Target Subjects and others involved in any insider-trading scheme constitutes relevant evidence of at least one of the Subject Offenses.

responsive records. Accordingly, the warrants requested herein will be transmitted to the Providers, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachments A and B to the proposed warrants.

23. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all messages within the Subject Accounts. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches may not work well for instant message data, where words are frequently written in shorthand. Moreover, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Orders

24. The existence and scope of this ongoing criminal investigation are not publicly known. As a result, premature public disclosure of this affidavit or the requested warrants could alert

potential criminal subjects that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. As is set forth above, the Target Subjects of this investigation are known to use computers and electronic communications in furtherance of their activity and thus could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation. *See* 18 U.S.C. § 2705(b)(3). From my experience investigating white-collar crime and securities fraud, I know that individuals who participate in such offenses may alert potential criminal subjects that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation.

25. Accordingly, there is reason to believe that, were the Providers to notify the subscriber or others of the existence of the warrants, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Providers not to notify any person of the existence of the warrants for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

26. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrants and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

27. Finally, based on my training and experience, I know that Google will request that the Government seek data related to email addresses with an enterprise domain such as @rocketonecapital.com and @mosaicist.com, which would include data relating to two of the

Subject Accounts, directly from the enterprises, pursuant to the U.S. Department of Justice Policy titled Seeking Enterprise Customer Data Held by Cloud Service Providers, December 2017, available at https://www.justice.gov/criminal-ccips/file/1017511/download. However, @rocketonecapital.com and @mosaicist.com appear to be owned or controlled by MICHAEL SHVARTSMAN and RAY CORRAL, respectively, both of whom are Target Subjects of this investigation. Because they are the apparent owners of the enterprises, notification would almost certainly mean they would be informed of the existence of this search warrant, which could cause them to delete, encrypt, or otherwise conceal the requested data. To the extent either enterprise has outside counsel (none is presently known to the Government), disclosure to outside counsel does not appear to be a viable option because, based on my understanding of professional responsibility rules, such counsel will be required to report such a disclosure to the client. Additionally, it is my understanding that certain materials requested from Google cannot be obtained directly from the enterprise because enterprise account users cannot access or download certain types of data, including the types of data requested for Subject Account-7 and Subject Account-8. Therefore, I respectfully request that the proposed order specifically require the Provider to produce enterprise data.

V. Conclusion

28. Based on the foregoing, I respectfully request that the Court issue the warrants sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C.

§ 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

s/Marc Troiano, by the Court, with permission

Marc Troiano
Special Agent
FBI

Sworn to before me this
10th day of February, 2022 by reliable electronic means
(FaceTime)

Honorable Debra Freeman
United States Magistrate Judge
Southern District of New York